



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10143695 A**(43) Date of publication of application: **29.05.98**

(51) Int. Cl.

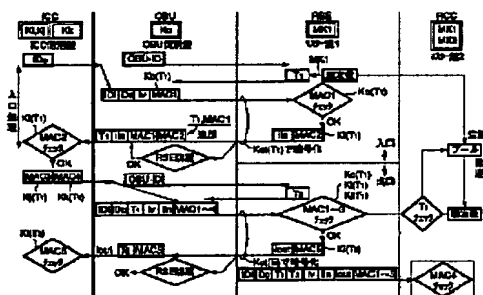
G07B 15/00**G07B 15/00****G06F 17/60****H04L 9/32**(21) Application number: **08305018**(22) Date of filing: **15.11.96**(71) Applicant: **TOSHIBA CORP**(72) Inventor:
KITAORI MASASHI
KAWAMURA SHINICHI
FUKAZAWA KAZUO
NAITO KAZUTOSHI(54) **MUTUAL AUTHENTICATION SYSTEM, TOLL
RECEIVING SYSTEM OF TOLL ROAD AND
MUTUAL AUTHENTICATION METHOD OF TOLL
RECEIVING SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To perform mutual authentication by using a cryptographic key by radio even though the communication speed of an IC card is slow and calculation capability is small and to receive toll by providing an IC read/write device which reads information of an IC card of a facility user and 1st and 2nd authentication devices which are installed at the entrance and exit of the facility.

SOLUTION: Communication between an IC card read/write device which is onboard unit (OBU) that is mounted on a passing vehicle and an entrance roadside system starts. When a passage ticket automatic issuing machine of the entrance roadside system recognizes the OBU, it gives passage permission to the vehicle. The passage ticket automatic issuing machine also sends a message authentication code that makes an IC card recognize as a correct roadside system. An exit traffic lane controller of an exit roadside system confirms a correct OBU, the same OBU at both entrance and exit and a legal IC card by confirming a message authentication code.

COPYRIGHT: (C)1998,JPO



【特許請求の範囲】

【請求項1】 施設利用者に所有されるＩＣカードに対して情報の読み取り、及び送信情報を書き込むＩＣカード読取書込装置と、施設の入口に設けられる第１の認証装置と施設の出口に設けられる第２の認証装置とから構成される相互認証システムにおいて、

上記第１の認証装置は、

上記ＩＣカード向けの認証情報と次に情報交換を行う第２の認証装置向けの認証情報とを生成する第１の生成手段と、

この第１の生成手段で生成された２つの認証情報を上記ＩＣカードに送信する第１の送信手段と、

上記ＩＣカードは、

上記ＩＣカード読取書込装置を介して上記第１の送信手段から送信された２つの認証情報を受信する第１の受信手段と、

この第１の受信手段で受信された２つの認証情報の内のＩＣカード向けの認証情報により認証を行う第１の認証手段と、

この第１の認証手段により認証された際、上記第２の認証装置向けの認証情報を生成する第２の生成手段と、

この第２の生成手段で生成された認証情報と上記第１の受信手段で受信された２つの認証情報の内の第２の認証装置向けの認証情報とを上記ＩＣカード読取書込装置を介して上記第２の認証装置に送信する第２の送信手段と、

上記第２の認証装置は、

上記第２の送信手段から送信された複数の認証情報により上記ＩＣカードの認証を行う第２の認証手段と、を具備したことを特徴とする相互認証システム。

【請求項２】 車両に搭載されるＩＣカードに対して情報の読み取り、及び送信情報を書き込むＩＣカード読取書込装置と、施設の入口に設けられる第１の認証装置と施設の出口に設けられる第２の認証装置とから構成される有料道路の料金収受システムにおいて、

上記第１の認証装置は、

上記ＩＣカード向けの認証情報と次に情報交換を行う第２の認証装置向けの認証情報とを生成する第１の生成手段と、

この第１の生成手段で生成された２つの認証情報と当該入口を示す入口情報とを上記ＩＣカードに送信する第１の送信手段と、

上記ＩＣカードは、

ＩＤ番号を含む課金情報を記憶する記憶手段と、

上記ＩＣカード読取書込装置を介して上記第１の送信手段から送信された２つの認証情報と入口情報とを受信する第１の受信手段と、

この第１の受信手段で受信された２つの認証情報の内のＩＣカード向けの認証情報により認証を行う第１の認証手段と、

この第１の認証手段により認証された際、上記第２の認証装置向けの認証情報を生成する第２の生成手段と、

この第２の生成手段で生成された認証情報と上記第１の受信手段で受信された２つの認証情報の内の第２の認証装置向けの認証情報と入口情報及び上記記憶手段に記憶されている課金情報とを上記ＩＣカード読取書込装置を介して上記第２の認証装置に送信する第２の送信手段と、

上記第２の認証装置は、

10 上記第２の送信手段から送信された複数の認証情報により上記ＩＣカードの認証を行う第２の認証手段と、

この第２の認証手段により認証できたとき、上記第２の送信手段から送信された入口情報及び課金情報に基づいて有料道路の通行料金の収受処理を行う収受手段と、を具備したことを特徴とする有料道路の料金収受システム。

【請求項３】 ＩＣカードの情報の読み取り、情報を書き込むＩＣカード読取書込装置と、少なくとも２つの認証装置とから構成される相互認証システムにおいて、

20 上記ＩＣカード読取書込装置と最初に情報交換を行う第１の認証装置が、

上記ＩＣカード向けの認証情報と次に情報交換を行う第２の認証装置向けの認証情報とを生成する第１の生成手段と、

この第１の生成手段で生成された２つの認証情報を上記ＩＣカードに送信する第１の送信手段と、

上記ＩＣカードが、

上記ＩＣカード読取書込装置を介して上記第１の送信手段から送信された２つの認証情報を受信する第１の受信手段と、

30 この第１の受信手段で受信された２つの認証情報の内のＩＣカード向けの認証情報により認証を行う第１の認証手段と、

この第１の認証手段により認証された際、上記第２の認証装置向けの認証情報を生成する第２の生成手段と、

この第２の生成手段で生成された認証情報と上記第１の受信手段で受信された２つの認証情報の内の第２の認証装置向けの認証情報とを上記ＩＣカード読取書込装置を介して上記第２の認証装置に送信する第２の送信手段と、

40 上記第２の認証装置が、

上記第２の送信手段から送信された複数の認証情報による認証を行う第２の認証手段と、

を具備したことを特徴とする相互認証システム。

【請求項４】 車両に設けられた車載機とこの車載機に挿入されるＩＣカードとから構成される車載機器と、上記車両が通過する入口と出口の路側システムとの間で料金収受が行われる料金収受システムの相互認証方法であって、

50 上記入口の路側システムがＩＣカード向けの認証情報と

出口の路側システム向けの認証情報とを生成して上記車載機に無線で送信し、上記車載機が送信された2つの認証情報を受信して上記ICカードに送信し、ICカードが送信された2つの認証情報の内のICカード向けの認証情報により認証し、認証された際、上記出口の路側システム向けの認証情報を生成し、生成した出口の路側システム向けの認証情報と上記車載機から送信された2つの認証情報の内の出口の路側システム向けの認証情報とを上記車載機に送信し、上記車載機が送信された2つの認証情報を受信して上記出口の路側システムに無線で送信し、上記出口システムが送信された2つの認証情報により認証するようにしたことを特徴とする料金収受システムの相互認証方法。

【請求項5】 車両に設けられた車載機とこの車載機に挿入されるICカードとから構成される車載機器と、上記車両が通過する路側システムとの間で無線によって料金収受が行われる料金収受システムにおいて、

上記車載機が、

ICカードが挿入された際、乱数を発生する乱数発生手段と、

この乱数発生手段で発生された乱数を上記挿入されたICカードに送信する第1の送信手段と、

上記ICカードが、

上記第1の送信手段から送信された乱数を受信する第1の受信手段と、

この第1の受信手段で乱数を受信された際、予め格納しているID番号を上記車載機に送信する第2の送信手段と、

上記第1の受信手段で受信された乱数と予め格納している相互認証プロトコルに用いる秘密鍵とを予め格納しているカード固有の暗号鍵で暗号化する暗号化手段と、

この暗号化手段で暗号化された暗号文を上記車載機に送信する第3の送信手段と、

上記車載機が、

上記第2の送信手段から送信されたID番号を受信する第2の受信手段と、

この第2の受信手段で受信されたID番号から予め格納しているマスタ鍵で秘密鍵を生成する生成手段と、

上記第3の送信手段から送信された暗号文を受信する第3の受信手段と、

この第3の受信手段で受信された暗号文を上記生成手段で生成された秘密鍵で復号化する復号化手段と、

この復号化手段で復号化された復号文の所定の位置に上記乱数発生手段で発生された乱数と同じ乱数があるか否かを確認する確認手段と、

この確認手段で同じ乱数が確認された際、上記復号化手段で復号化された復号文から相互認証プロトコルに用いる秘密鍵を取り出し、この相互認証プロトコルに用いる秘密鍵を用いて上記路側システムとの間で相互認証プロトコルを制御する制御手段と、

を具備したことを特徴とする料金収受システム。

【請求項6】 車両に設けられた車載機とこの車載機に挿入されるICカードとから構成される車載機器と、上記車両が通過する路側システムとの間で無線によって料金収受が行われる料金収受システムの相互認証方法であって、

上記車載機がICカードが挿入された際、乱数を発生し、発生された乱数を上記挿入されたICカードに送信し、上記ICカードが送信された乱数を受信し、乱数が受信された際、予め格納しているID番号を上記車載機に送信し、受信された乱数と予め格納している相互認証プロトコルに用いる秘密鍵とを予め格納しているカード固有の暗号鍵で暗号化し、暗号化された暗号文を上記車載機に送信し、上記車載機が送信されたID番号を受信し、受信されたID番号から予め格納しているマスタ鍵で秘密鍵を生成し、送信された暗号文を受信し、受信された暗号文を生成された秘密鍵で復号化し、復号化された復号文の所定の位置に上記発生された乱数と同じ乱数があるか否かを確認し、同じ乱数が確認された際、復号化された復号文から相互認証プロトコルに用いる秘密鍵を取り出し、この相互認証プロトコルに用いる秘密鍵を用いて上記路側システムとの間で相互認証プロトコルを制御するようにしたことを特徴とする料金収受システムの相互認証方法。

【請求項7】 車両に設けられた車載機とこの車載機に挿入されるICカードとから構成される車載機器と、上記車両が通過する路側システムとの間で無線によって料金収受が行われる料金収受システムにおいて、

上記車載機が、

ICカードが挿入された際、乱数を発生する乱数発生手段と、

この乱数発生手段で発生された乱数と予め格納している車載機固有の公開鍵と対応するデジタル署名とを上記挿入されたICカードに送信する第1の送信手段と、

上記ICカードが、

上記第1の送信手段から送信された乱数と車載機固有の公開鍵と対応するデジタル署名とを受信する第1の受信手段と、

この第1の受信手段で受信された車載機固有の公開鍵と対応するデジタル署名とから予め格納されている公開鍵を用いて復号化する第1の復号化手段と、

この第1の復号化手段で復号化された復号文のデジタル署名が正しいか否かを確認する確認手段と、

この確認手段で正しいと確認された際、上記第1の受信手段で受信された乱数と予め格納されているICカード固有の秘密鍵とを連結して上記復号文の車載機固有の公開鍵で暗号化する暗号化手段と、

この暗号化手段で暗号化された暗号文を上記車載機に送信する第2の送信手段と、

上記車載機が、

上記第2の送信手段で送信された暗号文を受信する第2の受信手段と、

この第2の受信手段で受信された暗号文を上記車載機固有の公開鍵に対応する車載機固有の秘密鍵で復号化する第2の復号化手段と、

この第2の復号化手段で復号化された復号文の所定の位置に上記乱数発生手段で発生された乱数と同じ乱数があるか否かを確認する確認手段と、

この確認手段で同じ乱数が確認された際、上記復号化手段で復号化された復号文から上記ICカード固有の秘密鍵を取り出し、このICカード固有の秘密鍵を用いて上記路側システムとの間で相互認証プロトコルを制御する制御手段と、

を具備したことを特徴とする料金収受システム。

【請求項8】 車両に設けられた車載機とこの車載機に挿入されるICカードとから構成される車載機器と、上記車両が通過する路側システムとの間で無線によって料金収受が行われる料金収受システムの相互認証方法であって、

上記車載機がICカードが挿入された際、乱数を発生し、発生された乱数と予め格納している車載機固有の公開鍵と対応するデジタル署名とを上記挿入されたICカードに送信し、上記ICカードが送信された乱数と車載機固有の公開鍵と対応するデジタル署名とを受信し、受信された車載機固有の公開鍵と対応するデジタル署名とから予め格納されている公開鍵を用いて復号化し、復号化された復号文のデジタル署名が正しいか否かを確認し、正しいと確認された際、受信された乱数と予め格納されているICカード固有の秘密鍵とを連結して上記復号文の車載機固有の公開鍵で暗号化し、暗号化された暗号文を上記車載機に送信し、上記車載機が送信された暗号文を受信し、受信された暗号文を上記車載機固有の公開鍵に対応する車載機固有の秘密鍵で復号化し、復号化された復号文の所定の位置に上記発生された乱数と同じ乱数があるか否かを確認し、同じ乱数が確認された際、上記復号化された復号文から上記ICカード固有の秘密鍵を取り出し、このICカード固有の秘密鍵を用いて上記路側システムとの間で相互認証プロトコルを制御するようにしたことを特徴とする料金収受システムの相互認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、例えば有料道路において、車両等の移動体に搭載されている車載機器と無線によって相互認証して料金収受を行う相互認証システムと有料道路の料金収受システムと料金収受システムの相互認証方法に関する。

【0002】

【従来の技術】従来、例えば有料道路における料金収受装置の端末装置を備える料金所において、有料道路本線

に入線する車両に対して料金所の入口の端末装置で入口情報（料金所の識別番号、車種、時刻等）を記録した通行券を発行し、上記料金所と有料道路で接続されている他の料金所の出口で、上記料金所で発行された通行券の入口情報により、この料金所の出口に備えられている端末装置を用いて通行料金を計算し、通行料金の収受を行っている。

【0003】この料金収受装置は、複数の端末装置を持って各料金所に設置されている。料金所の入口の各端末装置は、有料道路本線に入線する車両に対して入口情報（料金所の識別番号、車種、時刻等）を記録した通行券を発行する。料金所の出口の各端末装置は、通行料金計算のためのテーブル、例えば全ての料金所との区間料金、車種別の料金等をメモリに記憶しており、料金所の出口において料金所の入口で発行された通行券の入口情報によりメモリに記憶している通行料金テーブルを検索して通行料金を計算する。

【0004】それに対して、車両に搭載した車載機器と地上（料金所）側の通信装置と無線で料金の収受を行う料金収受システムが、非接触、ノンストップのメリットをユーザに提供する手段として注目を受けている。

【0005】有料道路における無線カード式の料金収受システムの場合、道路側に設置される路側機器と車両に搭載される車載機器との間で無線通信による課金情報の送受信が行われる。ここで、車載機器が支払請求先とは直接関係を持たない車載機と、支払請求先の情報を担ったICカードを用いた構成を想定する。

【0006】従来、ICカードを使った認証システムでは、通信されたメッセージの所有者（作者）を特定し、かつメッセージが改竄されていないことを確認するためにメッセージ認証コードと呼ばれる符号が使われている。これについて図13を用いて簡単に説明する。

【0007】送信者Aが作ったメッセージは通信手段によって受信者BにAが作成したメッセージとして伝えられたとする。もちろん、この間の送信路に何も問題なければ両者のメッセージは同一であり、また、通信路が一つに確定していればそれはまぎれもなくAが作ったメッセージであると言える。

【0008】しかし、一般の通信路ではこのような保証はなく、誰かがAを装ってメッセージを作ったり、また、Aが作ったメッセージを通信過程で何かが自分の都合のよいように改竄する恐れもある。したがって、Bは自分が受け取ったメッセージが確かにAが作ったものであり、かつ改竄されていないことを確認しなくてはならない。

【0009】このため送信者Aと受信者Bは、お互いに同じ情報（これを共通鍵と呼ぶ）を共有する。この鍵を用いてAさんはメッセージをハッシュ関数と呼ばれる関数によってメッセージ認証コード（MAC）を作成する。ハッシュ関数は、一方向性関数の一種であり、この

関数の結果から元の値を算出することがきわめて困難な関数である。例えば、MD5、SHAと呼ばれるアルゴリズムが良く知られている。

【0010】Aはこれをメッセージに添付してBに送信する。これを受け取ったBはAが行ったと同じ行程で同じ共通鍵を使って受け取ったメッセージのメッセージ認証コードを作成する。メッセージが改竄されていれば受け取ったメッセージ認証コードと自分が作成したメッセージ認証コードとが一致しない。また、Bが所有する共通鍵を共有するA以外にこれと一致するメッセージ認証コードを作成するのは極めて困難であるので、Bはこのメッセージの作者がAであると確認することができる。

【0011】これはBがAのメッセージの正当性を検査する一方の認証である。さて、ここでICカードがAであった場合、ICカードを差し込む装置がBとした場合、もし、このICカードが入退室に使われるならば、つまりICカードを認証する装置が確かにその場所にあるICカードを差し込んだ装置であるならば、認証は一方方向で十分である。

【0012】しかし、ネットワークなどを使った通信を用い、認証する相手が特定できない場合などは、一方方向では不十分であり、お互いがお互いを認証しあう相互認証が不可欠である。この場合、メッセージ認証コードを付けたメッセージを相互に交換することで容易に実現できることは明かである。

【0013】これを図に表すと図14のようになる。前述の手續きに従って、Aの要求によりBはAの正当性をメッセージ認証コードを検証することで認証する。次に認証結果をAに返し、AがBの正当性を認証コードを用いて検証する。しかる後に、相互の通信を行うのである。

【0014】近年、こういったICカードを用いた認証システムが多方面に用いられる試みが行われている。その中には、有料の高速道路の料金収受システムなども含まれる。この場合の料金収受システムの特徴としては、ICカードを搭載した車両が高速道路で入口および出口ゲートを通過する極めて短い時間内にICカードと、高速道路の入口および出口にある路側システムとの相互認証を行う点にある。

【0015】しかしながら、この相互認証方式を有料道路の料金収受システムなどに応用する場合には次の問題が生じる。まず、AすなわちICカードは、高速演算が望めないため、Bすなわち路側システムの認証を完全に行うことができない。従って、車両が入口の路側システムで相互認証手續きの通信を行って入口の路側システムを認証した結果行われる通信は、次の出口の路側システムまで待機させられる。そして、車両が出口を通過したとき、同様に出口の路側システムを認証する必要が生じ、これにも同様の時間が必要となるため、結局、入口路側システムと出口路側システムを完全に認証した後で

それに基づいた料金収受の通信を行うことが不可能となる。

【0016】また、路側システムとICカードとの間で容易に考えられる安全な課金方式としては、ICカードに個別の秘密の暗号鍵Kが格納されていて、路側システムはあらかじめICカードの識別番号から鍵Kを特定し、路側システムが車載機を介してICカードと暗号通信を行うことによって確かに正当なICカードを搭載した車であることを確認するとともに、そのカードから特定される対象者に課金を行うようなシステムがある。ここで、ICカードと路側システムが行う暗号通信とは、例えば次に示す4ステップからなる相互認証プロトコルである。

(1) 乱数R1をICカードが生成し、路側システムに送る。

(2) 路側システムは第2の乱数R2を生成し、R1とR2を連結したものを鍵Kで暗号化して、結果をICカードに送る。

(3) ICカードは受信した暗号文を鍵Kで復号し、

(1) で送ったのと同じR1が所定の形式で得られることを確認すると共に、復号文からR2を取り出して路側システムに送り返す。

(4) 路側システムは送り返された電文が、(2) で生成したR2と一致することを確認する。

【0017】このような手續きの相互認証プロトコルにより路側システムは、ICカードが路側システムと同じ鍵Kを持つことが確認できる。鍵Kは、カード毎に異なる値を発行するので鍵Kが特定できたことにより課金先が特定できたことになる。なお、この手續きを実施するためには路側システムがICカードと同じ鍵を持つことが必要であるが、路側システムは例えばカードの識別番号とそのカードに格納されている鍵のリストを所持したり、カード識別番号から秘密の変換アルゴリズムによって鍵を導き出す等の手段を用いることができる。

【0018】このような相互認証の手續きは、用いるICカードが高速の通信機能を有していれば容易に実装できる。しかしながら、ISOで規格化された標準的なコンタクト型ICカードの通信速度は9.6kbpsであり、車両が料金所(入口と出口の路側システム)をノンストップで通過する料金収受システムでは、上記のような相互認証プロトコルをICカードと路側システムとの間で直接行うことはできない。また、仮に通信速度が向上しても、ICカードに搭載されるプロセッサの計算能力は通常小さく、相互認証の暗号化演算をこの時間内で行うことは不可能である。

【0019】

【発明が解決しようとする課題】上記したように、車両に搭載されるICカードと有料道路の料金所(入口と出口の路側システム)との間で暗号鍵を用いて無線で料金の収受を行なう料金収受システムにおいては、ICカー

ドの通信速度が遅いので相互認証をすることができず、また、ＩＣカードの計算能力が小さいので相互認証の暗号化演算を時間内で行うことができないという問題があった。

【００２０】そこで、この発明は、ＩＣカードの通信速度が遅く、計算能力が小さくても暗号鍵を用いて無線で相互認証を行って料金の収受を行うことのできる相互認証システムと有料道路の料金収受システムと料金収受システムの相互認証方法を提供することを目的とする。

【００２１】

【課題を解決するための手段】この発明の相互認証システムは、施設利用者に所有されるＩＣカードに対して情報の読み取り、及び送信情報を書き込むＩＣカード読取書込装置と、施設の入口に設けられる第１の認証装置と施設の出口に設けられる第２の認証装置とから構成される相互認証システムにおいて、上記第１の認証装置は、上記ＩＣカード向けの認証情報と次に情報交換を行う第２の認証装置向けの認証情報とを生成する第１の生成手段と、この第１の生成手段で生成された２つの認証情報を上記ＩＣカードに送信する第１の送信手段と、上記ＩＣカードは、上記ＩＣカード読取書込装置を介して上記第１の送信手段から送信された２つの認証情報を受信する第１の受信手段と、この第１の受信手段で受信された２つの認証情報の内のＩＣカード向けの認証情報により認証を行う第１の認証手段と、この第１の認証手段により認証された際、上記第２の認証装置向けの認証情報を生成する第２の生成手段と、この第２の生成手段で生成された認証情報と上記第１の受信手段で受信された２つの認証情報の内の第２の認証装置向けの認証情報とを上記ＩＣカード読取書込装置を介して上記第２の認証装置に送信する第２の送信手段と、上記第２の認証装置は、上記第２の送信手段から送信された複数の認証情報により上記ＩＣカードの認証を行う第２の認証手段とから構成されている。

【００２２】この発明の有料道路の料金収受システムは、車両に搭載されるＩＣカードに対して情報の読み取り、及び送信情報を書き込むＩＣカード読取書込装置と、施設の入口に設けられる第１の認証装置と施設の出口に設けられる第２の認証装置とから構成される有料道路の料金収受システムにおいて、上記第１の認証装置は、上記ＩＣカード向けの認証情報と次に情報交換を行う第２の認証装置向けの認証情報とを生成する第１の生成手段と、この第１の生成手段で生成された２つの認証情報と当該入口を示す入口情報とを上記ＩＣカードに送信する第１の送信手段と、上記ＩＣカードは、ＩＤ番号を含む課金情報を記憶する記憶手段と、上記ＩＣカード読取書込装置を介して上記第１の送信手段から送信された２つの認証情報と入口情報とを受信する第１の受信手段と、この第１の受信手段で受信された２つの認証情報の内のＩＣカード向けの認証情報により認証を行う第１

の認証手段と、この第１の認証手段により認証された際、上記第２の認証装置向けの認証情報を生成する第２の生成手段と、この第２の生成手段で生成された認証情報と上記第１の受信手段で受信された２つの認証情報の内の第２の認証装置向けの認証情報と入口情報及び上記記憶手段に記憶されている課金情報とを上記ＩＣカード読取書込装置を介して上記第２の認証装置に送信する第２の送信手段と、上記第２の認証装置は、上記第２の送信手段から送信された複数の認証情報により上記ＩＣカードの認証を行う第２の認証手段と、この第２の認証手段により認証できたとき、上記第２の送信手段から送信された入口情報及び課金情報に基づいて有料道路の通行料金の収受処理を行う収受手段とから構成されている。

【００２３】この発明の相互認証システムは、ＩＣカードの情報の読み取り、情報を書き込むＩＣカード読取書込装置と、少なくとも２つの認証装置とから構成される相互認証システムにおいて、上記ＩＣカード読取書込装置と最初に情報交換を行う第１の認証装置が、上記ＩＣカード向けの認証情報と次に情報交換を行う第２の認証装置向けの認証情報とを生成する第１の生成手段と、この第１の生成手段で生成された２つの認証情報を上記ＩＣカードに送信する第１の送信手段と、上記ＩＣカードが、上記ＩＣカード読取書込装置を介して上記第１の送信手段から送信された２つの認証情報を受信する第１の受信手段と、この第１の受信手段で受信された２つの認証情報の内のＩＣカード向けの認証情報により認証を行う第１の認証手段と、この第１の認証手段により認証された際、上記第２の認証装置向けの認証情報を生成する第２の生成手段と、この第２の生成手段で生成された認証情報と上記第１の受信手段で受信された２つの認証情報の内の第２の認証装置向けの認証情報とを上記ＩＣカード読取書込装置を介して上記第２の認証装置に送信する第２の送信手段と、上記第２の認証装置が、上記第２の送信手段から送信された複数の認証情報による認証を行う第２の認証手段とから構成されている。

【００２４】この発明の料金収受システムの相互認証方法は、車両に設けられた車載機とこの車載機に挿入されるＩＣカードとから構成される車載機器と、上記車両が通過する入口と出口の路側システムとの間で料金収受が行われる料金収受システムの相互認証方法であって、上記入口の路側システムがＩＣカード向けの認証情報と出口の路側システム向けの認証情報とを生成して上記車載機に無線で送信し、上記車載機が送信された２つの認証情報を受信して上記ＩＣカードに送信し、ＩＣカードが送信された２つの認証情報の内のＩＣカード向けの認証情報により認証し、認証された際、上記出口の路側システム向けの認証情報を生成し、生成した出口の路側システム向けの認証情報と上記車載機から送信された２つの認証情報の内の出口の路側システム向けの認証情報とを上記車載機に送信し、上記車載機が送信された２つの認

証情報を受信して上記出口の路側システムに無線で送信し、上記出口システムが送信された2つの認証情報により認証するようにしたことを特徴とする。

【0025】この発明の料金收受システムは、車両に設けられた車載機とこの車載機に挿入されるICカードとから構成される車載機器と、上記車両が通過する路側システムとの間で無線によって料金收受が行われる料金收受システムにおいて、上記車載機が、ICカードが挿入された際、乱数を発生する乱数発生手段と、この乱数発生手段で発生された乱数を上記挿入されたICカードに送信する第1の送信手段と、上記ICカードが、上記第1の送信手段から送信された乱数を受信する第1の受信手段と、この第1の受信手段で乱数を受信された際、予め格納しているID番号を上記車載機に送信する第2の送信手段と、上記第1の受信手段で受信された乱数と予め格納している相互認証プロトコルに用いる秘密鍵とを予め格納しているカード固有の暗号鍵で暗号化する暗号化手段と、この暗号化手段で暗号化された暗号文を上記車載機に送信する第3の送信手段と、上記車載機が、上記第2の送信手段から送信されたID番号を受信する第2の受信手段と、この第2の受信手段で受信されたID番号から予め格納しているマスタ鍵で秘密鍵を生成する生成手段と、上記第3の送信手段から送信された暗号文を受信する第3の受信手段と、この第3の受信手段で受信された暗号文を上記生成手段で生成された秘密鍵で復号化する復号化手段と、この復号化手段で復号化された復号文の所定の位置に上記乱数発生手段で発生された乱数と同じ乱数があるか否かを確認する確認手段と、この確認手段で同じ乱数が確認された際、上記復号化手段で復号化された復号文から相互認証プロトコルに用いる秘密鍵を取り出し、この相互認証プロトコルに用いる秘密鍵を用いて上記路側システムとの間で相互認証プロトコルを制御する制御手段とから構成されている。

【0026】この発明の料金收受システムの相互認証方法は、車両に設けられた車載機とこの車載機に挿入されるICカードとから構成される車載機器と、上記車両が通過する路側システムとの間で無線によって料金收受が行われる料金收受システムの相互認証方法であって、上記車載機がICカードが挿入された際、乱数を発生し、発生された乱数を上記挿入されたICカードに送信し、上記ICカードが送信された乱数を受信し、乱数を受信された際、予め格納しているID番号を上記車載機に送信し、受信された乱数と予め格納している相互認証プロトコルに用いる秘密鍵とを予め格納しているカード固有の暗号鍵で暗号化し、暗号化された暗号文を上記車載機に送信し、上記車載機が送信されたID番号を受信し、受信されたID番号から予め格納しているマスタ鍵で秘密鍵を生成し、送信された暗号文を受信し、受信された暗号文を生成された秘密鍵で復号化し、復号化された復号文の所定の位置に上記発生された乱数と同じ乱数があ

るか否かを確認し、同じ乱数が確認された際、復号化された復号文から相互認証プロトコルに用いる秘密鍵を取り出し、この相互認証プロトコルに用いる秘密鍵を用いて上記路側システムとの間で相互認証プロトコルを制御するようにしたことを特徴とする。

【0027】この発明の料金收受システムは、車両に設けられた車載機とこの車載機に挿入されるICカードとから構成される車載機器と、上記車両が通過する路側システムとの間で無線によって料金收受が行われる料金收受システムにおいて、上記車載機が、ICカードが挿入された際、乱数を発生する乱数発生手段と、この乱数発生手段で発生された乱数と予め格納している車載機固有の公開鍵と対応するデジタル署名とを上記挿入されたICカードに送信する第1の送信手段と、上記ICカードが、上記第1の送信手段から送信された乱数と車載機固有の公開鍵と対応するデジタル署名とを受信する第1の受信手段と、この第1の受信手段で受信された車載機固有の公開鍵と対応するデジタル署名とから予め格納されている公開鍵を用いて復号化する第1の復号化手段と、この第1の復号化手段で復号化された復号文のデジタル署名が正しいか否かを確認する確認手段と、この確認手段で正しいと確認された際、上記第1の受信手段で受信された乱数と予め格納されているICカード固有の秘密鍵とを連結して上記復号文の車載機固有の公開鍵で暗号化する暗号化手段と、この暗号化手段で暗号化された暗号文を上記車載機に送信する第2の送信手段と、上記車載機が、上記第2の送信手段で送信された暗号文を受信する第2の受信手段と、この第2の受信手段で受信された暗号文を上記車載機固有の公開鍵に対応する車載機固有の秘密鍵で復号化する第2の復号化手段と、この第2の復号化手段で復号化された復号文の所定の位置に上記乱数発生手段で発生された乱数と同じ乱数があるか否かを確認する確認手段と、この確認手段で同じ乱数が確認された際、上記復号化手段で復号化された復号文から上記ICカード固有の秘密鍵を取り出し、このICカード固有の秘密鍵を用いて上記路側システムとの間で相互認証プロトコルを制御する制御手段とから構成されている。

【0028】この発明の料金收受システムの相互認証方法は、車両に設けられた車載機とこの車載機に挿入されるICカードとから構成される車載機器と、上記車両が通過する路側システムとの間で無線によって料金收受が行われる料金收受システムの相互認証方法であって、上記車載機がICカードが挿入された際、乱数を発生し、発生された乱数と予め格納している車載機固有の公開鍵と対応するデジタル署名とを上記挿入されたICカードに送信し、上記ICカードが送信された乱数と車載機固有の公開鍵と対応するデジタル署名とを受信し、受信された車載機固有の公開鍵と対応するデジタル署名とから予め格納されている公開鍵を用いて復号化し、復

号化された復号文のデジタル署名が正しいか否かを確認し、正しいと確認された際、受信された乱数と予め格納されているICカード固有の秘密鍵とを連結して上記復号文の車載機固有の公開鍵で暗号化し、暗号化された暗号文を上記車載機に送信し、上記車載機が送信された暗号文を受信し、受信された暗号文を上記車載機固有の公開鍵に対応する車載機固有の秘密鍵で復号化し、復号化された復号文の所定の位置に上記発生された乱数と同じ乱数があるか否かを確認し、同じ乱数が確認された際、上記復号化された復号文から上記ICカード固有の秘密鍵を取り出し、このICカード固有の秘密鍵を用いて上記路側システムとの間で相互認証プロトコルを制御するようにしたことを特徴とする。

【0029】

【発明の実施の形態】以下、この発明の一実施例について図面を参照して説明する。この発明に係る料金收受システムは、入口と出口の路側システムから構成される入口発券出口收受方式（以下、クローズドシステムと記述する）と、均一車線のみで構成されるオープンシステムとに分けられる。

【0030】また、詳しくは後述するが車両に搭載される車載機器は、無線通信機能や操作部、表示部を備えた車載機としてのオンボードユニット（On Board Unit：以下、OBUと記述する）2と利用者のID番号、口座番号（以下、課金情報と記述する）を備えたICカード1とから構成されている。

【0031】また、OBU2には、予め搭載する車両の車種を決定する要因の長さ・軸数・重量・用途・特長のデータ（以下、車両情報と記述する）が登録されている。ICカード1には、課金情報が記憶されている。

【0032】図1は、この発明の料金收受システムに係るICカード1の構成を示すものである。すなわち、ICカード1は、全体の制御を司るCPU10、制御プログラム等を記憶しているROM11、課金情報等を記憶するRAM12、乱数を発生する乱数発生器13、後述するセキュリティ方式Aまたセキュリティ方式Bのための鍵が格納される鍵格納エリア14、及び暗号化アルゴリズム実行器15とから構成されている。

【0033】図2は、OBU2の構成を示すものである。すなわち、OBU2は、全体の制御を司るCPU20、制御プログラム等を記憶しているROM21、車両情報等を記憶するRAM22、乱数を発生する乱数発生手段としての乱数発生器23、後述するセキュリティ方式Bのための鍵が格納される鍵格納エリア14、暗号化アルゴリズム実行器15、各車線に設置されたアンテナと通信を行うアンテナ26、アンテナ26の制御を行う無線通信制御部27、操作案内をする文字表示とLEDランプを備えた表示部28、複数のボタンを備えた操作部29、及びICカード1が装着されて読取り・書込みが可能なICカード処理部18とから構成されている。

【0034】図3は、路側システム（RSE）として、クローズドシステムに用いられる入口路側システムの構成を示すものである。すなわち、入口路側システムは、車両の進行方向から車種判別装置31、第1アンテナ32、通行券自動発行機30、発進検知装置33、及び第2アンテナ34とから構成されている。

【0035】車種判別装置31は、進入した車両を検知し、車両の進入を通行券自動発行機30に伝達する。さらに、進入した車両の車種を判別し、判定結果を通行券自動発行機30に通知する。

【0036】第1アンテナ32は、通行券自動発行機30の指示により、進入した車両に搭載された車載機器との通信を行うものである。発進検知装置33は、車両の発進を検知し、通行券自動発行機30に通知する。

【0037】第2アンテナ34は、第1アンテナ32で正常に交信が終了した車両が発進検知装置33に進入することにより、通行券自動発行機30の指示の元で、車載機器との通信を行うものである。

【0038】通行券自動発行機30は、各機器の制御を行うと同時に、車載機器を搭載していない車両（以下、非ETC車と記述する）に対して通行券を発行する。通行券自動発行機30にはネガティブリストが登録されている。

【0039】図4は、路側システム（RSE）として、クローズドシステムに用いられる出口路側システムの構成を示すものである。図4の（a）に示すように出口路側システムは、車両の進行方向から車両検知装置41、第1アンテナ42、出口ブース内機器43、車両検知装置44、及び第2アンテナ45とから構成されている。

【0040】出口ブース内機器43は、図4の（b）に示すように非ETC車が持参した通行券を処理する通行券確認機46、前納のカードを処理するカード処理機47、現金支払い車に対する領収書発行を行う領収書発行機48、各機器の制御を行う出口車線制御装置40とから構成されている。出口車線制御装置40は、ネガティブリストが登録されている。なお、通行券確認機46は、ICカード1を処理することのできるICカードリーダー46aを備えている。

【0041】車両検知装置41は、車両の進入を検知した結果を出口ブース内機器43の出口車線制御装置40に通知する。第1アンテナ42は、出口車線制御装置40の制御の元で、進入車両に搭載された車載機器との通信を行うものである。

【0042】車両検知装置44は、車両の進入を検知した結果を出口車線制御装置40に通知する。第2アンテナ45では、出口車線制御装置40の制御の元で、車両に搭載された車載機器との通信を行う。

【0043】図5は、路側システム（RSE）として、オープンシステムに用いられる均一路側システムの構成を示すものである。図5の（a）に示すように均一路側

システムは、車両の進行方向から車両検知装置51、第1アンテナ52、ブース内機器53、車両検知装置54、及び第2アンテナ55とから構成されている。

【0044】ブース内機器53は、図5の(b)に示すように料金支払種別や進入車両の車種を入力し、各機器の制御を行う料金処理機50、前納のカードを処理するカード処理機56、現金支払い車に対する領収書の発行を行う領収書発行機57、ICカード1を処理することのできるICカードリーダ58とから構成されている。なお、料金処理機50にはネガティブリストが登録されている。

【0045】車両検知装置51は、車両の進入を検知した結果をブース内機器53の料金処理機50に通知する。第1アンテナ52は、料金処理機50の制御の元で、進入車両に搭載された車載機器との交信を行うものである。

【0046】車両検知装置54は、車両の進入を検知した結果を料金処理機50に通知する。第2アンテナ55では、料金処理機50の制御の元で、車両に搭載された車載機器との交信を行う。

【0047】利用者は、車両に車載機器を搭載し、OBU2にICカード1を挿入した状態で走行する。OBU2に挿入されたICカード1は、OBU2の正当性を確認することにより、OBU2に対してカードID番号を通知する。

【0048】次に、クローズシステムの道路を利用する例について説明する。入口路側システムでは、車種判別装置31が車両の進入を検知することにより、通行券自動発行機30に進入検知を伝達する。通行券自動発行機30は、第1アンテナ32を制御し、進入する車両に搭載されている車載機器（ICカード1が挿入されたOBU2）に対する交信問い合わせを開始する。車載機器は、正当なアンテナからの問い合わせと認識することにより、予めICカード1から通知されたID番号とOBU2に記録されている車両情報を返信する。

【0049】通行券自動発行機30は、車載機器からの応答が正当と認識することにより、ICカード1のID番号をネガティブリストと照合し、正当であれば入口を特定する道路番号・料金所番号・通過年月日時分・車線番号（以下、入口情報Aと記述する）を車載機器に送信する。OBU2では、入口情報Aの受信が正常に行われたことを確認して、入口路側システムに受信完了を通知する。

【0050】入口路側システムは、車載機器からの受信完了を受けることにより、通行券自動発行機30に発券停止を指示し、正常な車載機器搭載車両（以下、ETC車と記述する）と認定する。

【0051】ETC車が発信検知装置33を通過することにより、通行券自動発行機30は、発信検知装置33から車両進入の通知を受け、第2アンテナ34を制御

し、車載機器に対する交信問い合わせを実行する。車載機器は、正当なアンテナからの問い合わせと認識することにより、予めICカード1から通知されたID番号を通知する。

【0052】通行券自動発行機30は、車載機器からの応答が正当と認識することにより、ICカード1のID番号を第1のアンテナ32で受信したものと比較し、一致していれば車種判別装置31から受信した車種判定結果を入口情報Bとして第2アンテナ34を利用して車載機器に返信する。

【0053】車載機器（ICカード1が挿入されたOBU2）では、入口情報Bのデータが正常に受信されたことを確認し、第2アンテナ34に受信完了を通知する。同時に車載機器では、正常に受信した入口情報Aと入口情報BとをICカード1に入口情報（入口情報Aと入口情報Bとを合わせたものを入口情報とする）として記録する。

【0054】出口路側システムでは、車両検知装置41が車両の進入を検知することにより、車両の進入を出口車線制御装置40に通知する。出口車線制御装置40では、第1アンテナ42を制御し、進入した車両に対して問い合わせを実行する。出口路側システムでも入口路側システム同様に相手の正当性を認識することにより、車載機器は、OBU2に記録されている入口情報及び課金情報を第1アンテナ42に伝送する。

【0055】出口車線制御装置40では、第1アンテナ42を経由して受信した入口情報を元に通行料金の算出を行い、同時にID番号のネガティブリスト照合を行い、ID番号の正当性を認識することにより、入口情報及び出口情報（料金所番号・通過年月日時分・車線番号・通行料金）を利用履歴として、OBU2に伝送する。OBU2では、利用履歴が正常に受信完了したことを確認し、路側システムに受信完了を通知する。同時に、ICカード1に対して利用履歴を記録する。

【0056】次に、オープンシステムの均一路側システムについて説明する。上述したクローズシステムと同様に利用者は、車両に車載機器を搭載し、OBU2にICカード1を挿入した状態で走行する。ICカード1は、OBU2の正当性確認を行い、ID番号を通知しておく。

【0057】均一路側システムでは、車両検知装置51が車両の進入を検知することにより、料金処理機50に車両進入を通知する。料金処理機50は、第1アンテナ52を制御し、車載機器に対して問い合わせを実行する。上述した入口車線と同様に相手の正当性を認識することにより、OBU2は、予め通知されたICカード1のID番号とOBU2に記録された車両情報を第1アンテナ52に送信する。

【0058】料金処理機50では、第1アンテナ52を経由して受信したID番号をネガティブリストと照合

し、正当性が認識された場合、車両情報を元にした車種判定が行われ、判定した車種で通行料金を算出する。算出結果を元に料金所情報（料金所番号・通過年月日時分・車線番号・通行料金）を生成し、利用履歴としてOBU2に伝送する。

【0059】OBU2では利用履歴が正常に受信完了したことを確認し、均一路側システムに受信完了を通知する。同時に、ICカード1に対して利用履歴を記録する。図6は、この発明に係る通行券自動発行機30の構成を示すものである。すなわち、通行券自動発行機30は、各機器と接続されて全体の制御を司るCPU301、制御プログラム等を記憶しているROM302、各種情報を記憶するRAM303、乱数を発生する乱数発生器304、後述するセキュリティ方式Aのための鍵が格納される鍵格納エリア305、暗号化アルゴリズム実行器306、及び通行券発行処理部307とから構成されている。

【0060】図7は、この発明に係る出口車線制御装置40の構成を示すものである。すなわち、出口車線制御装置40は、各機器と接続されて全体の制御を司るCPU401、制御プログラム等を記憶しているROM402、各種情報を記憶するRAM403、乱数を発生する乱数発生器404、後述するセキュリティ方式Aのための鍵が格納される鍵格納エリア405、及び暗号化アルゴリズム実行器406とから構成されている。

【0061】次に、このような構成において第1実施例について説明する。まず、利用者は車両に車載機器を搭載し、OBU2にICカード1を挿入した状態で走行する。ICカード1の鍵格納エリア14には、登録発行時に特定の数字（IC-ID）および3つの個別鍵（K_i、K_j、K_k）が格納されている。K_iおよびK_jは、IC-IDに路側システム固有鍵MK1を一方方向性関数を用いて作用させることによって生成する。

【0062】

$K_i = f(IC-ID, MK1) \dots\dots\dots (1)$

ただし $f()$ は一方方向性関数。

$K_j = g(IC-ID, MK1) \dots\dots\dots (2)$

ただし $g()$ は一方方向性関数。

【0063】また、K_kはIC-IDにカード発行局固有鍵MK2を一方方向性関数を用いて作用させることによって、K_i、K_j同様に生成する。

$K_k = h(IC-ID, MK2) \dots\dots\dots (3)$

ただし $h()$ は一方方向性関数。

【0064】一方方向性関数を用いることによって、ICカード1に格納されるK_i、K_j、K_kが不正に読まれたとしても、これらを導き出すのに用いられたシステム固有鍵MK1、MK2を逆算により求めることは不可能となるので本システム全体の安全性は保たれる。

$MAC1 = MAC(K0(T1), ICC-ID, OBU-ID, Iv) \dots\dots\dots (5)$

【0065】OBU2にもまた特定の数字（OBU-ID）と2つの個別鍵（K₀、K_{0t}）が鍵格納エリア4に格納されている。K₀はICカード1の個別鍵同様、OBU-IDに路側システム固有鍵MK1を一方方向性関数を用いて作用させたことによって生成する。

【0066】

$K0 = F(OBU-ID, MK1) \dots\dots\dots (4)$

ただし、 $F()$ は一方方向性関数。一方、K_{0t}は全てのOBU2に共通していて、路側システムにも与えられる情報であり、おもに通信路の暗号化鍵生成に用いられる。K₀、K_{0t}共に、それ自体はICチップの中に埋め込まれるか、あるいは既知の物理的手段によって、プローブ等で取り出すことが出来ないように保護されている。

【0067】ICカード1をOBU1に差し込んだとき、あるいはICカード1を差し込んだ後にOBU2に電源が投入されたとき、あるいはICカード1を差し込んだ後にOBU2の所定のスイッチもしくは所定の複数キーを入れたとき、あるいはOBU2が路側システムから所定の信号を受け取ったとき、ICカード1のIC-IDがOBU2に送信され格納される。

【0068】その後、IC-IDは、OBU2の電源が切断されたとしても既知のバックアップ手段によりOBU2内に保持される。付加機能として、OBU2にIC-ID情報の抹消を行う手段を設けること、およびバックアップの時間制限機能を設け、例えば電源切断状態が1日連続すればIC-ID情報を抹消するといった設定を可能とするのも有効である。

【0069】次に、車両が路側システム（RSE）の入口に達したときのOBU2と路側システム（RSE）との情報の流れを図8を参照して説明する。まず、最初に通過する車両に搭載されているOBU2と入口路側システムとの通信が開始される。

【0070】OBU2からOBU-IDが入口路側システムの通行券自動発行機30に送信され、続いて通行券自動発行機30からOBU2に疑似乱数（T1）が送信される。疑似乱数は、順次数もしくは時刻を示す数を路側システム固有鍵MK1で暗号化して生成される。使われた順次数もしくは時刻を示す数はホストとしてのICカード発行局（RCC）に通知される。

【0071】OBU2は、T1及びK₀からセッション鍵K₀（T1）を所定の関数を用いて生成する。OBU2は、ICカード1から受け取り保持しているIC-IDと、OBU2が格納しているOBU-IDおよび車両情報（Iv）について、K₀（T1）を用いてメッセージ認証コード（MAC1）を生成する。

【0072】

ただし、 $MAC(k, |I|)$ はメッセージ I について k を鍵としたメッセージ認証関数である。

【0073】さらに OBU2 は、 $T1$ 及び $K0t$ から通信のためのセッション鍵 $K0t$ ($T1$) を所定の関数を用いて生成する。 $IC-ID$ 、 $OBU-ID$ 、 Iv 、及び $MAC1$ は $K0t$ ($T1$) を鍵として暗号化され、通行券自動発行機 30 に送信される。

【0074】通行券自動発行機 30 では、OBU2 から受け取った $OBU-ID$ と路側システム固有鍵 $MK1$ から式 4 を用いて $K0$ を算出すると共に、全ての OBU2 に共通な $K0t$ と OBU2 に送信した $T1$ から所定の関数により $K0t$ ($T1$) を算出する。受け取った情報は $K0t$ ($T1$) を鍵として暗号化されているので、路側システムの通行券自動発行機 30 はこれを直ちに解いて情報を取り出すことができる。

【0075】つぎに通行券自動発行機 30 は、OBU2 が付けた $MAC1$ を検証する。これには、OBU2 が行ったと同様の手続きをセッション鍵 $K0t$ ($T1$) を用いてメッセージ認証コードを生成し、これと OBU2 から受け取った $MAC1$ とが一致することを確認する。一致していれば、メッセージすなわち $IC-ID$ 、 $OBU-ID$ 、 Iv が全て正しい情報であることが確認できると共に、メッセージ認証に用いたセッション鍵が、通行券自動発行機 30 がその場で生成した乱数 $T1$ に基づい *

$$MAC2 = MAC(Ki(T1), MAC1, Iin) \dots\dots\dots (6)$$

ただし、 $MAC(k, |I|)$ はメッセージ I について k を鍵としたメッセージ認証関数である。

【0078】これを入口情報と共に OBU2 に暗号化して送信する。このときの暗号化鍵は受信時と同様 $K0t$ ($T1$) を用いる。OBU2 は、これを受け取り $K0t$ ($T1$) を鍵として暗号メッセージを解く。うまく解ければこのメッセージを発行したのは間違いなく $K0t$ を知り、先ほど $T1$ を送信してきた相手、すなわち正当な路側システム (通行券自動発行機 30) であることが確認できる。これによって、OBU2 は路側システム (通行券自動発行機 30) を認証することができるのである。

【0079】OBU2 は、OBU 固有鍵を使った路側システムの認証は行わない。ただすべての OBU2 に共通な鍵 $K0t$ と乱数 $T1$ を用いた通信路暗号化が正しければ、路側システムは正当と認証する。このことは不正な路側システムを構築された場合、比較的簡単に ($K0t$ が盗まれたなら) OBU2 に不正な入口情報がインプットされるのではないと思われる。しかし本システムでは、これについては問題ないと考えられる。なぜなら、たとえ不正な入口情報をインプットされたとしても、路側システム固有鍵 $MK1$ が盗まれない限り、正しい $MAC2$ を生成することができないからである。 $MAC2$ は※

$$MAC3 = MAC(Kj(T1), MAC2) \dots\dots\dots (7)$$

ただし、 $MAC(k, |I|)$ はメッセージ I について

*て作られているので、入口にさしかかった OBU2 がメッセージ認証コードを正しく生成したと言うことが確認できる。これはメッセージが盗聴などされ時間差を置いて 2 度使われるという、いわゆるリプレイ攻撃を阻止するのに非常に重要なポイントである。そしてこれによって通行券自動発行機 30 は OBU2 を認証することができるのである。

【0076】通行券自動発行機 30 が OBU2 を認証した時点で、OBU2 を搭載した車両は通行許可が与えられる。しかし、通行券自動発行機 30 は OBU2 へ正しい入口情報を送信しなければならないし、また、決済を行う IC カード 1 に対して自分が正しい路側システムであることを認証させるために IC カード 1 の鍵に基づくメッセージ認証コードを送信しなければならない。

【0077】このため、OBU2 から受け取ったメッセージが正しいことが確認できると、路側システムの通行券自動発行機 30 は、 $IC-ID$ と路側システム固有鍵 $MK1$ から式 1 に基づき IC カード固有鍵の一つ Ki を生成する。さらに Ki と乱数 $T1$ から所定の関数から Ki ($T1$) を生成する。そして入口情報 (Iin : 入口名称、時刻、車両情報など) および $MAC1$ について Ki ($T1$) を用いてメッセージ認証コード ($MAC2$) を生成する、

※OBU2 では確認されないが IC カード 1 の中で確認され、その情報が出口路側システムで確認されるため、こういった不正は必ず出口で検出できる。

【0080】次に、IC カード 1 内での処理と出口処理について説明する。正しい路側システムとして入口路側システム (通行券自動発行機 30) から受け取った入ロデータ (Iin)、乱数 ($T1$) 及びメッセージ認証コード ($MAC2$) は、IC カード 1 と OBU2 間の所定のインターフェースを通して IC カード 1 へ送られる。 $MAC2$ は、路側システム (通行券自動発行機 30) が IC カードの個別鍵 Ki を用いて作成したコードである。従って、IC カード 1 は路側システムと同様の手続きで、個別鍵 Ki を用いてメッセージ認証コードを作成し、これを $MAC2$ と比較する。一致すれば、この入口情報は IC カード 1 の個別鍵を知り得る正当な路側システムが作った情報であることが確認でき、これによって IC カードは路側システムを認証できる。

【0081】続いて IC カード 1 は、 $MAC2$ に対して二つの個別鍵 Kj 、 Kk と乱数 $T1$ を用いてそれぞれメッセージ認証コード ($MAC3$ および $MAC4$) を生成し、これを OBU2 に送信する。

【0082】

k を鍵としたメッセージ認証関数である。

【0083】

MAC4=MAC(Ki(T1)、MAC3)……………(8)

ただし、MAC(k、|I|)はメッセージIについてkを鍵としたメッセージ認証関数である。

【0084】OBU2はこれを出口まで保持する。もちろんこれらの情報についても、IC-IDの保持に用いるバックアップ機能及び、バックアップ制限機能は有効に作用し、ICカード1を抜いても、OBU2の電源が遮断されても情報は失われることはないし、またあらかじめ設定した時間に達したり、所定の操作によって情報を消去することも可能である。

【0085】出口では、まずOBU2はOBU固有値(OBU-ID)を出口路側システム(RSE)の出口車線制御装置40に送信し、出口車線制御装置40はOBU2に疑似乱数T2を送信する。OBU2は、所定の関数により暗号通信のためのセッション鍵K0t(T2)を生成する。続いてOBU2は、ICカード固有値(IC-ID)、OBU固有値(OBU-ID)、疑似乱数(T1)、およびこれまで用いた全てのメッセージ認証コード(MAC1、MAC2、MAC3、MAC4)を、K0t(T2)を鍵として暗号化し、出口車線制御装置40に送信する。

【0086】出口車線制御装置40では、K0t(T2)を鍵として暗号を解いた後、4つのメッセージ認証コードの内3つを一つ一つ確認する。まず、MAC1を確認することでOBU2がOBU個別鍵K0をもつ正当なOBU2であることと、入口および出口で同じOBU2であることを確認する。続いて、MAC2を確認することで入口情報が改竄された情報でなく正当な路側システムにおける入口路側システムの通行券自動発行機30が生成した情報であることを確認する。さらに、MAC3を確認することで、この入口情報が路側システム(通行券自動発行機30)が認識したICカード1が、入口通過中または直後にOBU2に挿入されていたことを確認する。

【0087】全てが正しく認証されるとOBU2は、疑似乱数T1の元になった順次数もしくは時間数を、路側システム固有鍵MK1を鍵として複号することによって得る。路側システム(RSE)において、入口路側システムの通行券自動発行機30からICカード発行局(RCC)へ登録された順次数は、数日間の後れをもって出口路側システムの出口車線制御装置40に配送されRAM403にテーブル化されている。

【0088】出口車線制御装置40がRAM403のテーブルを参照し、もしT1がこのテーブル上にあれば、OBU2が出口路側システムの出口車線制御装置40に送信した情報は不自然に古い、すなわち入口から出口に達するまで異常と推定できる時間を要していると判断できるので、この情報は不正にコピーされ再利用されていると考えられるので、その場合は認証できないものとし

て、本システム以外の所定の手続きにまわることになる。

【0089】認証が終了すると出口車線制御装置40は、所定のプログラムにより金額を決定し、この課金情報およびOBU2から受け取った全ての情報をICカード発行局(RCC)へ送信する。

【0090】続いて、出口車線制御装置40は、KiとT2から所定の関数によりKi(T2)を計算し、これを鍵として課金情報にメッセージ認証コード(MAC5)を生成し、OBU2にK0t(T2)を鍵として暗号化し送信する。

【0091】OBU2は、受け取った情報をK0t(T2)を鍵として複号化し、入口同様正しく復号できれば正当な路側システム(出口車線制御装置40)として認証できる。そして受け取った情報をICカード1に送信する。ICカード1は、課金情報に付けられたメッセージ認証コード(MAC5)により、出口車線制御装置40からの情報の正当性を検証し、認証できれば課金情報をログとしてICカード1内に保管する。

【0092】さて、ICカード発行局(RCC)では、出口路側システムの出口車線制御装置40から受け取った情報を全てのメッセージ認証コードを検証することによりチェックし、所定金融機関に対して課金通知を行うとともに、疑似乱数生成に使用した順次数または時刻数を登録する。これらは一度使用されたものであるので二度と使用されてはいけなものである。したがって使用済みとして登録された順次数は速やかに路側システムにおける各出口路側システムの出口車線制御装置40にネガティブリストとして配布される。これにより、情報の不正な二重使用を実質的に排除することができる。

【0093】次に、第2実施例について説明する。第2実施例における方式は、路側システムの料金所(入口路側システム)進入前に、事前にOBU2にICカード1の課金情報を送信が可能な方式で以下に説明する。この時、ICカード1とOBU2との間の通信路を保護しておかなければICカード固有の秘密の鍵Kが第三者に知られる可能性が非常に高くなる。そこで、本発明は、ICカード1とOBU2との間の通信路を保護し、ICカード固有の鍵KをOBU2に安全に転送する手段が最も重要である。

【0094】ここで、以下に考えられるいくつかの方法を提示する。

(1) ICカードをOBUに取り込み、データの送受信中は取り出せないようにする。

(2) 秘密鍵を用いる方式

(3) 公開鍵を用いる方式

上記(1)の方式については既知の技術で対応可能である。

【0095】次に、(2)の秘密鍵を用いる方式について説明する。図9は、発行局におけるICカード発行時の秘密鍵を示すものである。すなわち、あらかじめICカード1には、カード発行時にカードID番号からマスター鍵KMと所定の秘密鍵暗号アルゴリズムに基づいて導き出された鍵KiがICカード1の鍵格納エリア14に記憶されている。さらにICカード1には、前記鍵Kiとは異なる相互認証プロトコルに用いるための鍵Kansとが鍵格納エリア14に記憶されている。OBU2にも外部からは読めない形で共通のマスター鍵KMが鍵格納エリア24に記憶されている。

【0096】OBU2のCPU20では、ICカード処理部18でICカード1の挿入を検知することにより、ICカード1とのデータ送受信を開始するが、データ送受信を行う前にセキュリティ上は相互認証を行う必要がある。

【0097】そこで、OBU2とICカード(ICC)1との相互認証動作を図10を参照して説明する。まず、OBU2のCPU20は、乱数発生器23により乱数R1を発生させ、これをICカード1に送信する。また、ICカード1のCPU10は、鍵格納エリア14に記憶されているID番号をOBU2に送信する。

【0098】さらにICカード1のCPU10は、鍵格納エリア14に記憶されているID番号及び鍵Kansと乱数R1を連結してこれを鍵Kiで暗号化アルゴリズム実行器15を用いて暗号化し、この暗号文K(R1+Kans)をOBU2に送信する。

【0099】OBU2のCPU20は、受信したID番号からマスター鍵KMと所定の秘密鍵暗号アルゴリズムに基づいて暗号化アルゴリズム実行器25で鍵Kiを生成し、Kiを用いてICカード1から受信した暗号文K(R1+Kans)を復号化する。CPU20は、復号文の所定の位置にICカード1に送信した乱数と同じ乱数が存在することを確認する。もし同じ乱数が確認できなければ、OBU2のCPU20は処理NGとする。

【0100】同じ乱数が確認された後、OBU2のCPU20は、鍵Kansが正しく受信できたものとして復号文から鍵を取り出し、その鍵を用いて路側システムとの間で相互認証プロトコルを実施する。

【0101】次に、(3)の公開鍵を用いる方式について説明する。まず、ICカード1は、鍵Kと本方式に共通の公開鍵PKがICカード発行時点でICカード1の鍵格納エリア14に記憶されている。

【0102】図11は、発行局におけるOBU2発行時の暗号鍵を示すものである。すなわち、OBU2には、OBU固有の秘密鍵SKsと秘密鍵と対をなす公開鍵PKsとが鍵格納エリア24に記憶されている。また、この公開鍵PKsには、本方式に共通の秘密鍵SKでデジタル署名DSsが付けられている。OBU固有の秘密鍵SKsは、外部から読めない形で記憶されている。

【0103】ここで、OBU2とICカード(ICC)1との相互認証動作を図12を参照して説明する。まず、OBU2のCPU20は、乱数発生器23により乱数を生成し、これと鍵格納エリア24に記憶したOBU固有の公開鍵PKsと対応するデジタル署名DSsをICカード1に送る。

【0104】ICカード1のCPU10は、まず、添付されてきたデジタル署名が正しいものであることを本方式に共通の公開鍵PKで確認する(復号化)。PKs=PKsが確認できなかった場合は処理NGとして異常終了する。PKs=PKsが確認できてOBU2の正当性の確認が完了した場合、CPU10は、鍵Kと乱数R1を連結して、これをOBU固有の公開鍵PKsで暗号化アルゴリズム実行器25を用いて暗号化し、暗号文PKs(R1+K)をOBU2に送信する。

【0105】OBU2のCPU20は、この暗号文PKs(R1+K)をOBU固有の秘密鍵SKsで復号化し、所定の場所にOBU2が送信したのと同じ乱数R1が記録されていることを確認する。R1=R1が確認できなかった場合、CPU20は処理NGとする。

【0106】R1=R1が確認できて完了した場合、OBU2のCPU20は、鍵Kが正しく受信完了したのとして復号文から鍵Kを取り出し、その鍵Kを用いて路側システムとの間で相互認証プロトコルを実施する。

【0107】以上説明したように上記発明の実施の形態によれば、第1実施例では、ICカードの処理能力不足を補うため、入口と出口の路側システムの間で時間的な余裕を生み出すことにより、ICカードの認証を可能とした。この場合、クローズドシステムとしての入口発券出口収受方式に適用可能である。

【0108】また、第2実施例では、ICカードとOBUとの間の通信路を保護し、ICカード固有の鍵をOBUに安全に転送し、本来のICカードと路側システムとの間で行うべき相互認証のプロトコルのICカードの役割をOBUに代行させ、OBUと路側システムとの間で高速な伝送処理を可能とした。この場合、オープンシステムの均一路側システムに適用可能である。

【0109】

【発明の効果】以上詳述したようにこの発明によれば、ICカードの通信速度が遅く、計算能力が小さくても暗号鍵を用いて無線で相互認証を行って料金の収受を行うことのできる相互認証システムと有料道路の料金収受システムと料金収受システムの相互認証方法を提供することができる。

【図面の簡単な説明】

【図1】この発明の料金収受システムに係るICカード1の構成を示すブロック図。

【図2】OBUの構成を示すブロック図。

【図3】クローズドシステムに用いられる入口路側システムの構成を示す図。

25

【図4】クローズドシステムに用いられる出口路側システムの構成を示す図。

【図5】オープンシステムに用いられる均一路側システムの構成を示す図。

【図6】通行券自動発行機の構成を示す図。

【図7】出口車線制御装置の構成を示す図。

【図8】ICカードとOBUと路側システムとの間の情報の流れを説明するための図。

【図9】発行局におけるICカード発行時の秘密鍵を示す図。

【図10】OBUとICカードとの相互認証動作を説明するための図。

【図11】発行局におけるOBU発行時の暗号鍵を示す図。

【図12】OBUとICカードとの相互認証動作を説明するための図。

【図13】メッセージ認証コードを使用した認証システムを説明するための図。

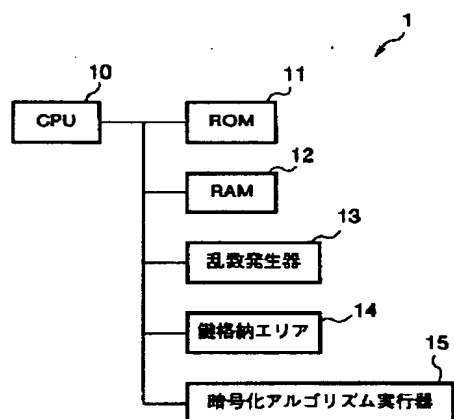
26

【図14】メッセージ認証コードを使用した相互認証システムを説明するための図。

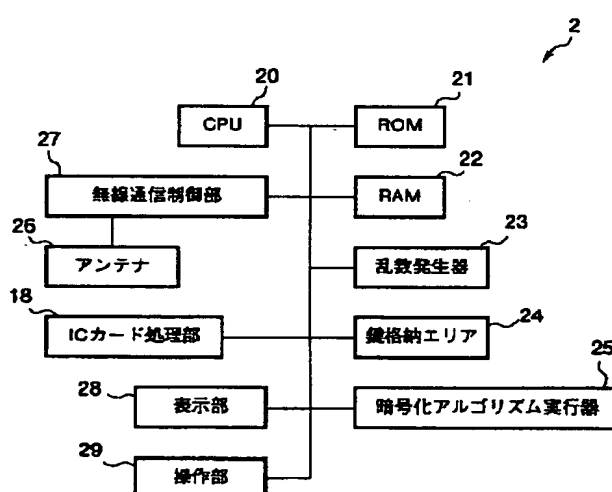
【符号の説明】

- 1…ICカード
 2…OBU (On Board Unit)
 10、20、301、401…CPU
 11、21、302、402…ROM
 12、22、303、403…RAM
 13、23、304、404…乱数発生器
 14、24、305、405…鍵格納エリア
 15、25、306、406…暗号化アルゴリズム実行器
 30…通行券自動発行機
 40…出口車線制御装置
 43…出口ブース内機器
 RSE…路側システム
 RCC…ICカード発行局

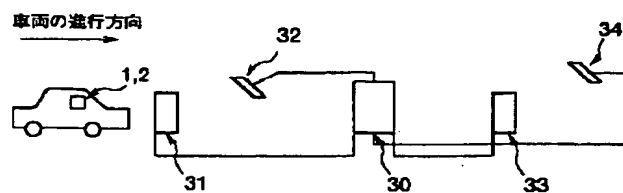
【図1】



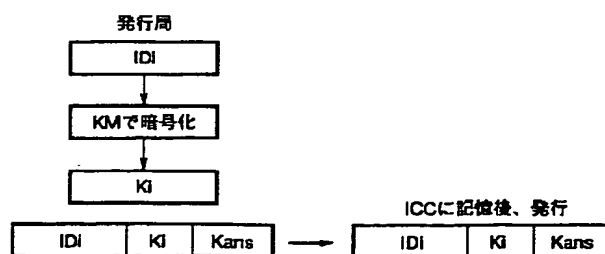
【図2】



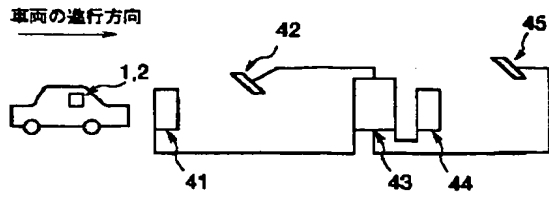
【図3】



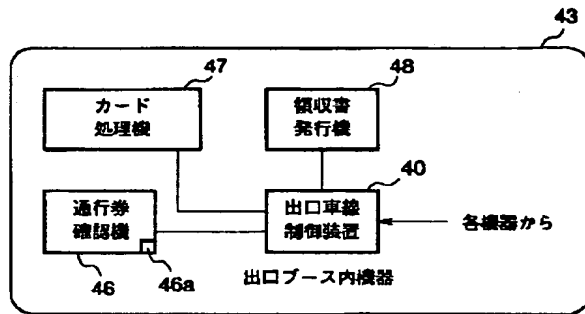
【図9】



【図4】

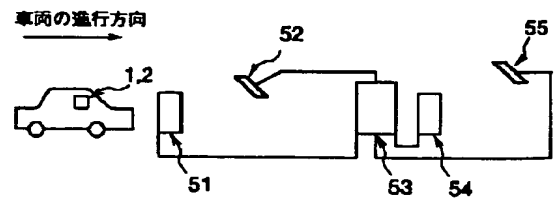


(a)

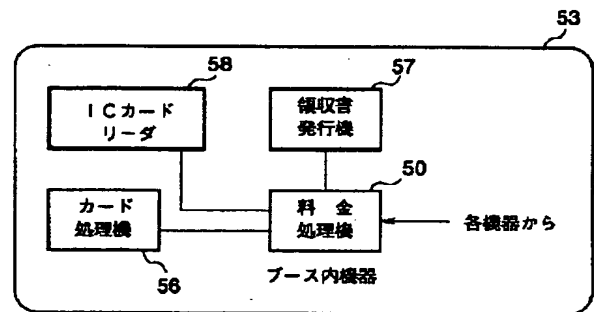


(b)

【図5】

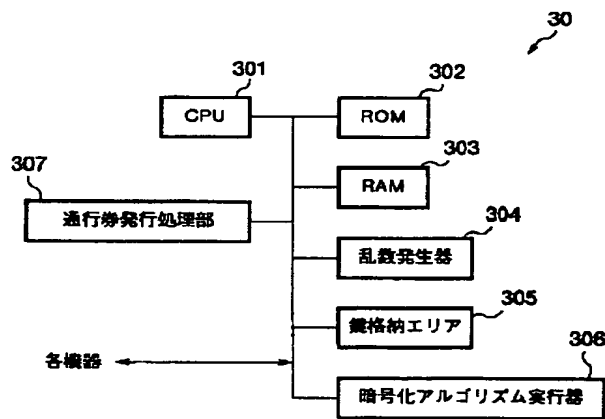


(a)

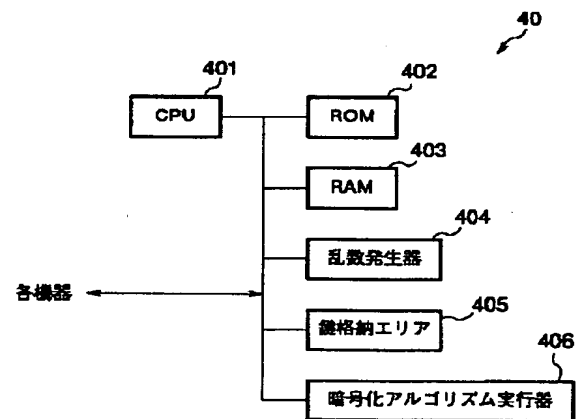


(b)

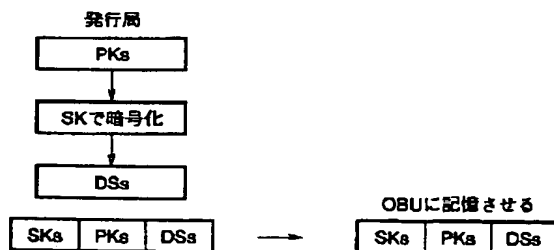
【図6】



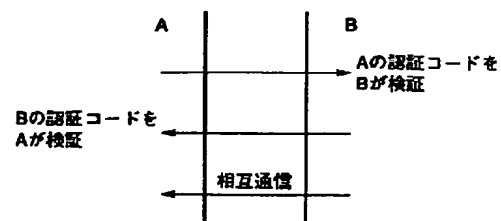
【図7】



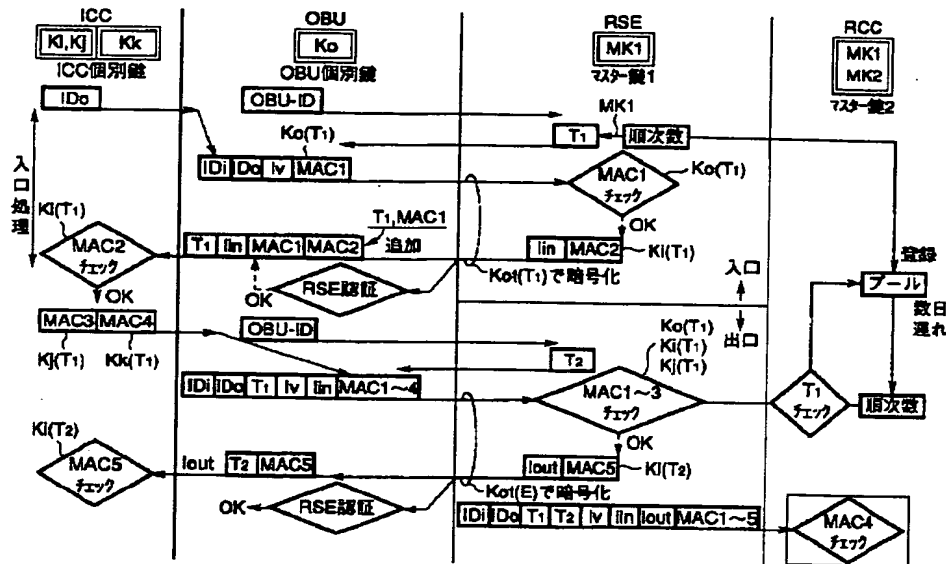
【図11】



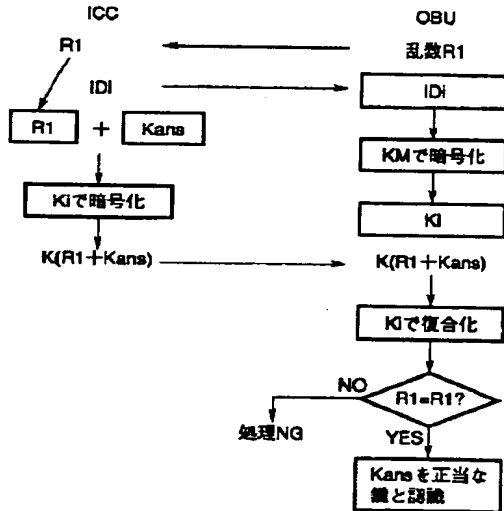
【図14】



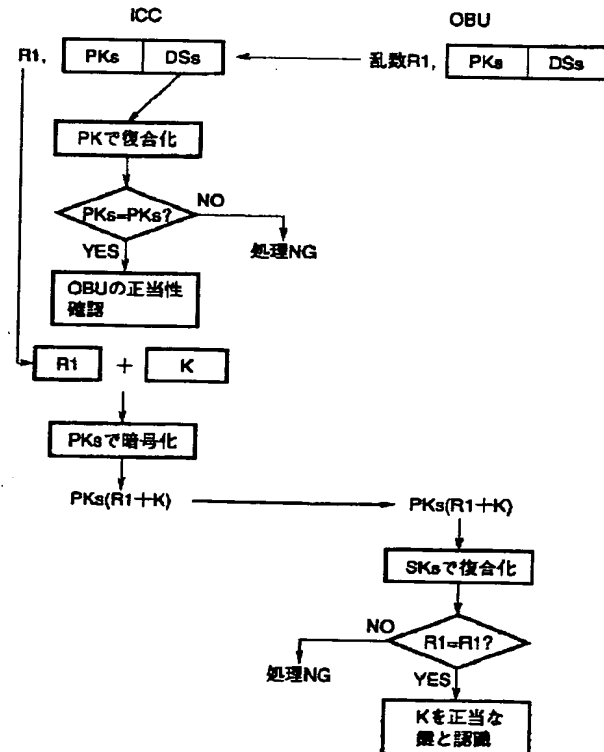
【図8】



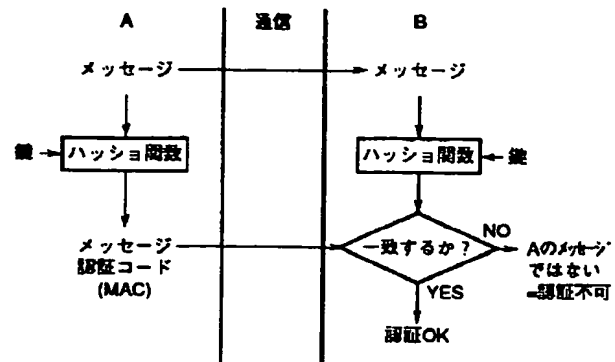
【図10】



【図12】



【図13】



フロントページの続き

(72) 発明者 内藤 一敏

東京都港区芝浦一丁目1番1号 株式会社

東芝本社事務所内